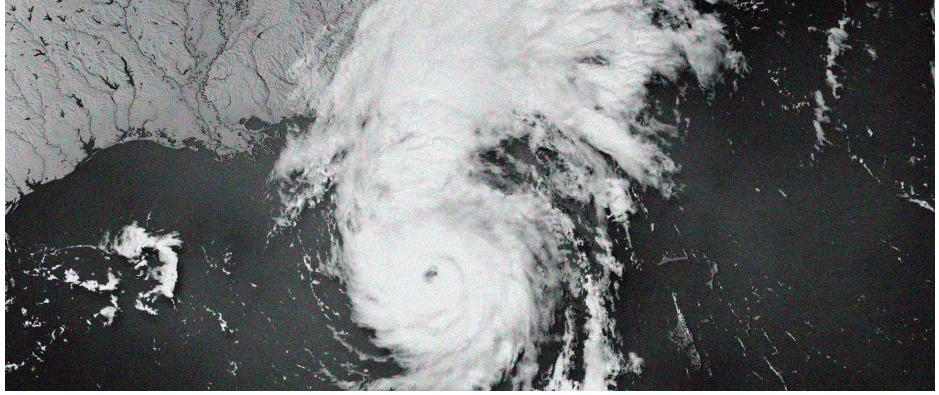
eBook

MÁS ALLÁ DE LA RECUPERACIÓN ANTE DESASTRES

Por qué necesitas una estrategia diferente cuando ocurren ciberataques.

Commvault®



Tu Enfoque para la Recuperación → Comienza Aquí

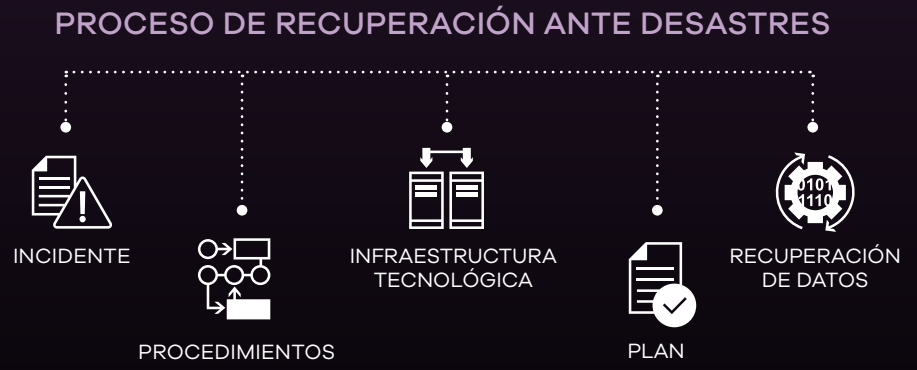
Desde eventos climáticos hasta ciberataques maliciosos, no faltan eventos destructivos que amenazan las operaciones de tu negocio en estos días. Nuestras fuentes de noticias están llenas de historias de daños causados por huracanes y ransomware.

Como parte de cualquier buena práctica de continuidad empresarial, necesitas un plan para que tu organización pueda recuperarse rápidamente después de un incidente. Deberás centrarte en proteger a tus empleados, a tus clientes y a todos tus datos, mientras mitigas el daño a tus activos, finanzas y reputación. Sin embargo, mantener la resiliencia frente a estas amenazas requiere vigilancia. La recuperación ante desastres y la ciberrecuperación no son lo mismo, por lo que es crucial entender las diferencias. Sigue leyendo para descubrir por qué necesitas tener ambos tipos de planes de recuperación en tu arsenal – y descubre cómo definir la viabilidad mínima en tu organización es una parte clave de la ciberrecuperación. Con una preparación exhaustiva, una estrategia de pruebas completa realizada regularmente y soluciones para la rápida recuperación y reconstrucción de todas tus aplicaciones y datos, estarás preparado para superar los desafíos de la recuperación.

Recuperación ante Desastres

Necesitas un plan de recuperación ante desastres para manejar eventos predecibles como fallos de hardware o desastres naturales como incendios e inundaciones. En general, estos incidentes no son intencionales y no atacan activamente tus datos.

La recuperación ante desastres generalmente sigue un plan predefinido con pasos establecidos para restaurar los sistemas rápidamente. Restaurar desde copias de seguridad te ayuda a volver a estar online, incluso si se pierde algún dato. Este proceso busca mantener el negocio continuo, minimizar el impacto a largo plazo y proteger los datos críticos.



Ciberrecuperación

En contraste, la ciberrecuperación aborda ataques maliciosos como el ransomware o las violaciones de datos, donde los atacantes intentan activamente dañar tus sistemas y corromper tus datos.

Esto podría afectar a un subconjunto de datos o a toda la infraestructura, incluyendo el sitio de conmutación por error de recuperación ante desastres.

Los ciberataques a menudo implican una investigación y una remediación antes de la recuperación, lo que puede extender el tiempo necesario. Necesitas contener el ataque y confirmar que no queden explotaciones. Cada elemento de tu entorno, desde el hardware hasta los datos y las copias de seguridad, debe ser examinado para detectar infecciones antes de restaurar, ya que los atacantes pueden haber ocultado malware o alterado los archivos de copia de seguridad. Deberás minimizar el daño, prevenir la pérdida de datos y mantener la postura de seguridad.

Vuelve a la actividad con la Viabilidad Mínima

Cuando un ciberataque deja a tu organización fuera de juego, la presión está en recuperar las operaciones lo más rápido posible para minimizar el daño financiero y reputacional. Por lo tanto, un aspecto importante de la recuperación cibernética es definir la viabilidad mínima de tu empresa, es decir, el conjunto mínimo de sistemas, datos y procesos que necesitas recuperar para seguir operando después de una interrupción.

01 Identificar activos críticos

Comienza identificando tus activos más críticos: sistemas (infraestructura, aplicaciones críticas para la misión, herramientas de comunicación); datos (operativos, de cumplimiento, de copia de seguridad); y procesos (operaciones comerciales, TI y seguridad, engagement con clientes).

02 Evaluar el impacto de una interrupción.

Una vez que hayas identificado estos activos, tendrás que evaluar el impacto de una interrupción en cada uno de ellos. ¿Cuánto cuesta a tu organización no estar operativa? Comprender los efectos del tiempo de inactividad en cada uno de tus activos críticos es vital para la toma de decisiones y para ayudar a priorizar su recuperación.

03 Crear un plan

A continuación, necesitas crear un plan para restaurar tus activos más críticos en caso de una interrupción, y probar, probar, probar. Asegúrate de que tus empleados estén capacitados en su papel en la recuperación.

04 Centrarse en una recuperación limpia y validada.

Finalmente, es importante señalar que debes validar que estás recuperando una copia limpia de tus datos; tener copias aisladas (air-gapped) ayudará a habilitar una recuperación más rápida de esos datos. Y debes realizar análisis forenses en una sala de recuperación aislada para encontrar la causa raíz y ayudar a prevenir futuros ataques.

Conoce el impacto de una interrupción:

$4.88M

Coste promedio de una brecha de seguridad

$14.056

Coste promedio de cada minuto de inactividad[2]

24 DÍAS

El tiempo de inactividad promedio después de un ataque de ransomware[3]

1 Informe sobre el costo de una filtración de datos 2024, IBM
2 Interrupciones de TI: costos y contención en 2024, Asociación de Gestión Empresarial
3 Statista

Preparación para Ciberrecuperación. Ámbito de Diseño

ESCENARIOS

La ciberrecuperación generalmente conduce a un conjunto diferente de necesidades en comparación con los planes de recuperación ante desastres/continuidad del negocio

Estas estrategias pueden combinarse para convergir recursos y procesos.

ELEMENTOS	RECUPERACIÓN ANTE DESASTRES / CONTINUIDAD DEL NEGOCIO	CIBERRECUPERACIÓN
COMPROMISO	Pérdida total de operaciones del sitio	Datos, redes, seguridad
RECUPERACIÓN	Commutación por error/ recuperación RTO, reconstrucción	Restauración selectiva para reparar
RECURSOS	Pila de disponibilidad completa	Validación, restauración, reconstrucción
PLANIFICACIÓN	Persistente	Elástica

ORGANIZACIÓN

La ciberrecuperación implica una responsabilidad compartida y colaborativa a lo largo de toda la organización (personas y procesos).

Integrar y automatizar las notificaciones, acciones informadas y flujos de trabajo sin interrupciones entre los equipos puede acelerar los resultados.

CAPABILIDADES

Los requisitos de una ciberrecuperación dependen de los objetivos de la organización.

- Copia de seguridad en bóvedas seguras, aisladas e inmutables
- Detección temprana de patrones sospechosos
- Análisis cibernético y saneamiento de datos
- Validación automatizada de la recuperación
- Recuperación planificada y rápida

Las Pruebas de Recuperación ante Desastres No Son Suficientes

Las pruebas de recuperación ante desastres son importantes, pero la ciberrecuperación es mucho más completa. Aunque ambos buscan restaurar la funcionalidad operativa después de interrupciones, las diferencias fundamentales requieren respuestas distintas. Los planes tradicionales de recuperación ante desastres luchan por abordar eficazmente las amenazas sutiles y las complejidades que presentan los ciberataques.

Aquí tienes por qué:

Por lo tanto, aunque los planes de recuperación ante desastres proporcionan una base valiosa para la respuesta a incidentes, confiar en ellos frente a un ciberataque puede ser peligroso. Un plan de ciberrecuperación dedicado, respaldado por herramientas especializadas, personal y pruebas frecuentes, es esencial para mitigar los riesgos y complejidades específicos de estos ataques maliciosos.

Las Pruebas de Ciberrecuperación Son Críticas

Las pruebas de ciberrecuperación es una práctica real (o prueba operativa) de restaurar una aplicación y sus datos a partir de una copia de seguridad. Este es el tipo de proceso de restauración que ocurrirá en un incidente cibernético, y es el proceso que recomienda NIST.1 La prueba de recuperación ante desastres y la prueba de ciberrecuperación tienen su lugar para escenarios aplicables, pero la ciberrecuperación es mucho más completa.

La prueba de ciberrecuperación permite la resiliencia de tus sistemas y datos, así como el negocio continuo. Recuperar aplicaciones y datos críticos está llena de complejidades y problemas. Probar la ciberrecuperación ayuda a descubrir errores y resolverlos cuando el riesgo es bajo.

La prueba dará a tus equipos la práctica y la confianza necesarias para recuperar aplicaciones y datos críticos cuando ocurra un incidente cibernético.

De hecho, NIST recomienda que "se realicen, protejan, mantengan y prueben copias de seguridad de los datos", porque "es mejor identificar un problema inesperado durante las pruebas que durante un evento cibernético real".[2] Sin embargo, la realidad es que muy pocas organizaciones prueban completamente, con frecuencia y con éxito.

NÚMEROS CRÍTICOS

194 DÍAS
Tiempo promedio que un atacante permanece en una empresa[2]

Los atacantes comienzan a moverse de manera lateral dentro de

48 MINUTOS
de un ataque[3]

82% DE LAS EMPRESAS
que pagan el rescate no recuperan todos sus datos[4]

1 https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf
2 https://www.ibm.com/reports/data-breach
3 https://go.crowdstrike.com/2025-global-threat-report.html
4 https://www.hiscoxgroup.com/news/blog/hiscox-cyber-readiness-report-2024

Cómo Commvault Puede Ayudarte

CON COMMVAULT, PUEDES:

- Proteger datos críticos con copias aisladas (air-gapped)
- Probar con frecuencia para confirmar que tu plan funciona y que tus empleados saben qué hacer.
- Validar que estás recuperando una copia limpia de tus datos.
- Realizar análisis forenses en un entorno de recuperación aislado y seguro.

LA GESTIÓN DE IDENTIDADES Y ACCESOS ES VITAL PARA RESTAURAR TUS OPERACIONES DESPUÉS DE UN ATAQUE:

Commvault Cloud for Active Directory Enterprise Edition:

te permite proteger y acelerar la recuperación de datos de AD ante la corrupción, la eliminación accidental y los ataques de ransomware, habilitando la recuperación automática a nivel de bosque.

Commvault® Cloud Cleanroom™ Recovery Cleanroom™

proporciona un entorno de recuperación seguro y aislado bajo demanda. Esta solución es más que un espacio seguro. Permite a las organizaciones probar la efectividad de sus planes de ciberrecuperación, entregar una recuperación limpia y rápida de tus aplicaciones y datos, y realizar un análisis forense seguro. Con almacenamiento inmutable aislado, automatización incorporada y escalado de recuperación mejorado por IA, Cleanroom Recovery te ayuda a mantener operaciones comerciales continuas, incluso frente a amenazas cibernéticas sofisticadas.

Commvault® Cloud Rewind™

va más allá de la copia de seguridad y la recuperación ante desastres tradicionales. Te permite descubrir, proteger, recuperar y reconstruir continuamente para establecer ciberresiliencia y mantener operaciones comerciales continuas. Puedes retroceder a un punto específico en el tiempo y reconstruir rápidamente aplicaciones dinámicas y distribuidas en la nube a partir de interrupciones y ataques de ransomware. Con una máquina del tiempo en la nube de doble bóveda patentada, puedes restaurar rápidamente tus datos, aplicaciones y configuraciones.

Aunque un plan de recuperación ante desastres es esencial para proteger la infraestructura de tu empresa, no estarás completamente protegido a menos que también cuentes con un plan de ciberrecuperación y una estrategia de pruebas. Esto es crucial para mantener tanto tus datos como tu reputación seguros frente a ciberataques.

Conoce más sobre cómo Commvault puede ayudar a proteger tu organización y obtén una demo de Commvault® Cloud Cleanroom™ Recovery y Cloud Rewind

commvault.com | 888.746.3849 | get-info@commvault.com

Commvault®